International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Graphical Password Authentication Using Colour Login Technique

Bhumika Patel[1], Amaan Sarwar[2], Prof. Sachin Chavan[3]

[1,2]Student, Dept. of Computer Engineering, M.G.M College of Engineering and Technology, Kamothe, Maharashtra, India
[3]Professor, Dept. of Computer Engineering, M.G.M College of Engineering and Technology, Kamothe, Maharashtra, India

---

Abstract - *Authorization is the technique of allowing only authorized personnel to have access to an account or data. With our world advancing in technology, new authentication techniques have been proposed. Alphanumeric Passwords being the traditional methods of the authorization technique it is widely adopted around the globe. Users tend to use similar alphanumeric passwords for every one of their accounts putting all their accounts at risk to breaching. These traditional passwords are vulnerable to the most common and easiest attack which is Shoulder Surfing Attack. The Shoulder Surfing is an assault which can be can be performed by unapproved user to acquire the approved user's password by looking from the user's shoulder when he enters his password. In a Jam-Packed place, these passwords can be seen over from the users shoulder easily. Not just in a crowded area but also when an attacker uses a camera or a zooming in device from a distance to look at the user's password. If the user keeps his password simple for them to remember, the password becomes easier to guess for the attacker too and if the password set it difficult to guess by the attacker it can easily be forgotten by the user. Biometrics and Graphical Passwords are utilized to defeat these issues related with the traditional authorization technique of Alphanumeric Password method, which assures safety of user's account and data. In this paper we have proposed a Graphical Password System using Colour Scheme in combination with Alphanumeric Password.*

Key Words: Graphical Password, Shoulder Surfing, *Alphanumeric Passwords*, Biometrics, Colour Scheme.

1. INTRODUCTION

Human factors are sometimes regarded as a computer security system's weakest component. Authentication, security operations, and designing stable systems are three major areas where human and computer interaction is essential, according to Patrick et al. [11]. Password theft is common. In Fact, one of the initially recorded instances of password burglary happened right back in 1962. When Individuals can't recall their passwords, they resort to methods like jotting it down, marginally transforming them or reusing them.

Data is the most precious entity of a user. To protect it we must need to provide best suited authorization system. The use traditional alphanumeric passwords for a system in which the user might login in a crowded place, the user's password can be prone to shoulder surfing attack. According to a recent Computerworld news article, the security team at a large company ran a network password cracker and within 30 seconds, they identified about 80% of the passwords [8].

Colours and images help user remember better as Psychology studies have revealed [2]. Many graphical password systems have been proposed which uses images and colours. These systems can be classified in three type:

1. *Recognition-Based System*
2. *Recall-Based System*
3. *Cued-Recall Based System*

To avoid shoulder surfing and to allow the user to use their traditional way of using text password, we propose an improved text based graphical password by utilizing colours. In short to integrate the text-based password and colours.

2. PROBLEM STATEMENT

Users are used to alphanumeric passwords. Though in our world where we are surrounded by the people and cameras, traditional alphanumeric password authentication without being a victim to shoulder surfing is not easy. Hence a system that can solve the problem of shoulder surfing by also using the alpha numeric password is needed.

3. LITERATURE SURVEY

In 1996, the first graphical password was introduced by Greg Blonder [16]. It required the user to asked to click on several locations on the image to create a password. To login the user must click on the same locations or close to those locations.

In 2002, to reduce the shoulder surfing attack, Sobrado and Birget [9] proposed three shoulder surfing resistant graphical password schemes, the Movable Frame scheme, the Intersection scheme, and the Triangle scheme [12]. The movable frame and intersection scheme fail frequently at authentication in 2006, to overcome the drawbacks of Sobrado and Birgets Scheme, the Convex Hull Click Scheme (CHC) is proposed by Wiedenbeck et al. It was designed to overcome the drawbacks of the triangle scheme. But scheme Convex-Hull Click has long login time [4].

Zhao et al. [6] introduced an alphanumeric shoulder surfing resistant graphical password as the user are not used to a purely graphical password. It is called S3APS which was a bit complex.

In 2009, shoulder surfing resistant graphical password in combination with colours was proposed by Gao et al. [5]. Colour passwords are intended to capitalize on this human characteristic in hopes that by reducing the memory burden on users, coupled with a larger full password space offered by colours, more secure passwords can be produced and users will not resort to unsafe practices in order to cope [2].

4. EXISTING SYSTEMS

Current authentication methods can be divided into:

1. Multi-Factor Authentication:

Multi-Factor Authentication (MFA) is an authentication method that requires two or more independent ways to identify a user. Models incorporate codes created from the client's cell phone, Captcha tests, fingerprints, or facial acknowledgment. MFA validation techniques and advancements increment the certainty of user by adding various layers of safety. MFA might be a decent protection against most record hacks, yet it has its own entanglements. Individuals may lose their telephones or SIM cards and not have the option to produce a confirmation code.

2. Biometric Authentication:

Biometrics authentication is a security process that depends on the natural unique qualities of a person. Here are key benefits of utilizing biometric authentication:

a. Biological qualities can be handily compared with the features saved in a data set.
b. Biometric authentication can handle actual access when introduced on entryways and entryways.
c. You can add biometrics into your multi-factor authentication process.

Biometric verification innovations are utilized by shoppers, governments and private partnerships including air terminals, etc. Common biometric verification strategies include:

a. Facial Recognition
b. Fingerprint scanners
c. Eye scanners
d. Voice recognition

3. Token-Based Authentication:

Token-based validation Systems enable users to enter their accreditations once and get an encrypted string in return. You would then be able to utilize the token to get to protected systems rather than entering your accreditations once more. The digital token proves that you already have access permission. Use cases of token-based authentication include RESTful APIs that are used by multiple frameworks and clients.

4. Knowledge-Based Authentication:

The alphanumeric passwords are the knowledge-based password. There are a lot of passwords to remember as a single user can have multiple accounts across the internet. Thus, numerous clients pick comfort over security and utilize straightforward passwords as opposed to making dependable passwords since they are simpler to recall. Basically, passwords have a ton of shortcomings and are not adequate in ensuring on the web data. Hackers can easily guess user credentials by running through all possible combinations until they find a match. Graphical passwords are also fall under this classification which can further be classified as:

1. *Recognition-Based System:* This method requires user to select the images that they recognize selecting during the registration process.

Dhamija and Perrig [13] (Fig - 1)proposed a recognition-based technique using the Hash Visualization technique [14], which required user to select the images that he chose during the registration period in the same order.

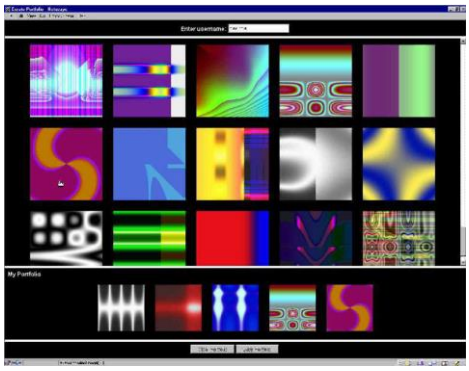


Fig - 1: Dhamija and Perrig's Random Images [13]

Akula and Devisetty's algorithm [10] was developed using hash function SHA-1, Sobrado and Birget [9] developed recognition-based shoulder surfing resistant schemes.

2. *Recall-Based System*: This category is very easy and convenient, but it seems that users can hardly remember their passwords. Still, it is more secure than the recognition-based technique [3].

Jermyn, et al. [15] proposed a technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password. A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are

stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space [8].

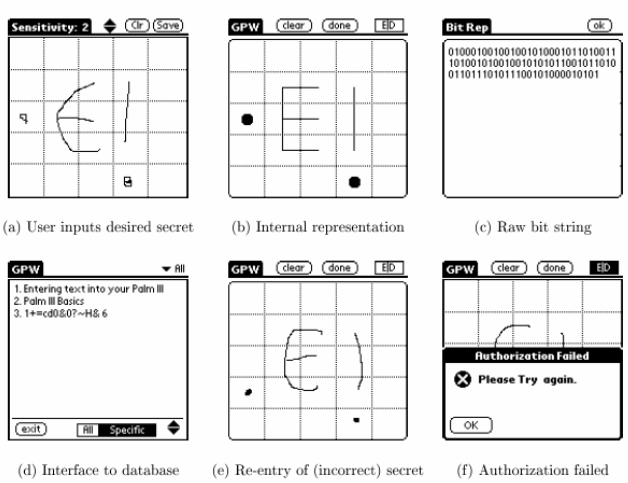


Fig - 2: Draw-a-Secret (DAS) technique proposed by Jermyn, et al. [15]

3. Cued-Recall Based System: In this category, users are provided with reminders or hints. Reminders help the users to reproduce their passwords or help users to reproduce the password more accurately. This is similar to recall-based schemes but it is recall with cueing [3].

Blonder [16] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password) [8].

5. PROPOSED SYSTEM

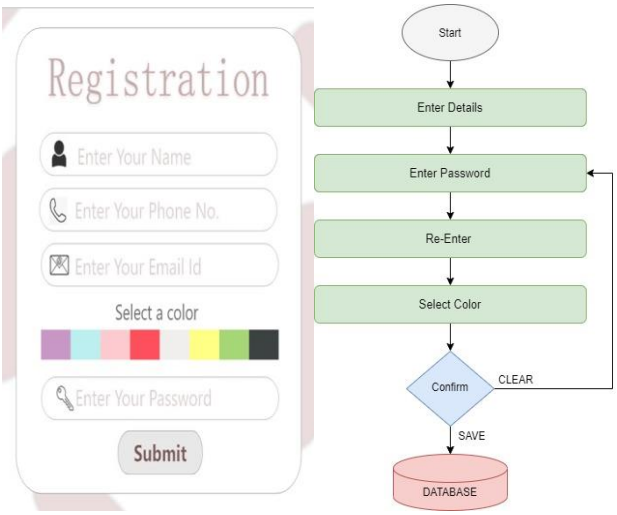
In the proposed system, the user can without much of a stretch and proficiently log into the system. Next, we break down the security and convenience of the proposed plan, and show the obstruction of the proposed plan to shoulder surfing and unplanned login.

To use the proposed system, user needs to initially enroll himself into this system by recording up the fundamental form for information. Overview of the proposed system is as follows:

- This proposed system involves Enrollment and the login phase.
- First phase being the enrollment phase.
- The enrollment phase contains colour choice (8 colours) and password section. The password can only contain 16 characters (8 Alphabets (a-f), 8 decimal digits (1-8)).
- After a successful enrollment, user can get to the login phase where he/she needs to initially verify their record by entering the email id which was entered while enrollment.
  When the email id is confirmed, the user may continue with graphical secret password area where he/she need to choose the characters related with the shading (colour).
- When the user is verified, he/she will be diverted to their profile page.

1. Enrollment Phase:

The user needs to set his passcode K of length L (4<L<8) characters, and pick one colour as his pass-shading from 8 colours appointed by the system. The leftover 7 colours not picked by the user are his imitation colours (let us call them decoy colours). The user needs to enroll an email address for re-enabling his record. The enrolment stage ought to continue in an environment free of shoulder surfing. The system then stores the user's textual passcode in the user's entrance in the secret key table, which should be encrypted by the system.



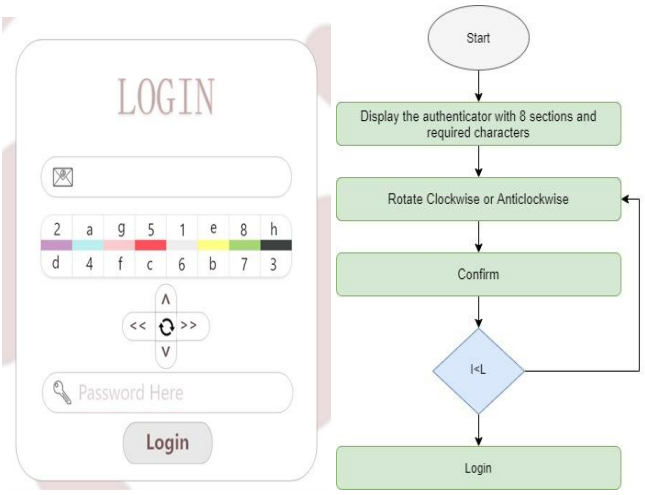
(a) **(b)**

Fig – 3(a): Registration Phase Design
Fig – 3(b): Registration Phase Flowchart

2. Login Phase:

The user solicitations to login the system, and the system shows a hover made out of 8 similarly estimated areas. The shades of the 8 areas are unique, and every area is distinguished by the shade of its bend, e.g., the red area is the area of red segment. At first, 16 characters are set moderately and haphazardly among these areas. All the showed characters can be at the same time pivoted into either the nearby area clockwise by tapping the "clockwise"

button once or the adjoining area counter clockwise by tapping the "counter clockwise" button once.



(a) **(b)**

Fig – 4(a): Registration Phase Design
Fig – 5(b): Registration Phase Flowchart

6. CONCLUSION

The primary point of proposing this authorization technique is to secure every user account from external threats which we never know when they tail or share our private information. This authorization technique makes sure that the user entities like documents, data, device etc.is bolted utilizing this Graphical Password System.

REFERENCES

[1] Towseef Akram, Vakeel Ahmad, Israrul Haq, Monisa Nazir, "Graphical Password Authentication," in International Journal of Computer Science and Mobile Computing, Vol.6 Issue.6, June- 2017.

[2] Aayush Dilipkumar Jain, Ramkrishna Khetan, Krishnakant Dubey, Prof. Harshali Rambade, "Color Shuffling Password Based Authentication," in International Journal of Engineering Science and Computing, April 2017, Volume 7 Issue No.4.

[3] Dhanashree Kadu, Shanthi Therese, Anil Chaturvedi, "Different Graphical Password Authentication Techniques," in International Conference on Emanations in Modern Technology and Engineering (ICEMTE) Volume: 5, Issue: 3 (March -2017).

[4] Prof. S. K .Sonkar, Prof. R.L .Paikrao, Prof. Awadesh Kumar, Mr. S. B.Deshmukh, 2014, "Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme, "in INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 03, Issue 02 (February 2014),

[5] H. Gao, X. Liu and R. Dai, "Design and analysis of a graphical password scheme," in Proc. of 4th Int. Conf. on Innovative Computing, Information and Control, Dec. 2009, pp. 675-678.

[6] H. Zhao and X. Li, "S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme", Proc. of 21st Int. Conf. on Advanced Information Networking and Applications Workshops, vol. 2, May 2007, pp. 467-472.

[7] B. Hartanto and S. Welly, "The usage of graphical password as a replacement to the alphanumerical password", Informatika, vol. 7, no. 2, 2006, pp. 91-97.

[8] Suo, Xiaoyuan & Zhu, Ying & Owen, G. (2005)." Graphical Passwords: A Survey". 463-472. 10.1109/CSAC.2005.27.

[9] J.C. Birget, "Shoulder-surfing resistant graphical passwords", Draft, 2005.

[10] S. Akula and V. Devisetty, "Image Based Registration and Authentication System", in Proceedings of Midwest Instruction and Computing Symposium, 2004.

[11] A. S. Patrick, A. C. Long, and S. Flinn, "HCI and Security Systems," presented at CHI, Extended Abstracts (Workshops). Ft. Lauderdale, Florida, USA., 2003.

[12] L. Sobrado "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4,2002

[13] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000

[14] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[15] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Passwords," in Proceedings of the 8th USENIX Security Symposium, 1999.

[16] G. E. Blonder, "Graphical passwords," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.